(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
29 décembre 2004 (29.12.2004)

PCT

(10) Numéro de publication internationale
WO 2004/114229 A1

(51) Classification internationale des brevets[7] : G07F 7/10

(21) Numéro de la demande internationale :
PCT/EP2004/051198

(22) Date de dépôt international : 22 juin 2004 (22.06.2004)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
03014209.5 25 juin 2003 (25.06.2003) EP

(71) Déposants *(pour tous les États désignés sauf US)* : **NAGRACARD S.A.** [CH/CH]; Route de Genève 22, CH-1033 Cheseaux-sur-Lausanne (CH). **SWISSCOM MOBILE AG** [CH/CH]; Schwarztorstrasse 61, CH-3050 Berne (CH).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **KSONTINI, Rached** [CH/CH]; Route Aloys Fauquez 26, CH-1004 Lausanne (CH). **JOLY, Stéphane** [CH/CH]; Crêt-Dessus, CH-1098 Epesses (CH). **CANTINI, Renato** [IT/CH]; Route du Moulin 35, CH-1782 Belfaux (CH). **TAZI, Mehdi** [CH/CH]; Av. de Croix-Rive 5, CH-1028 Préverenges (CH).

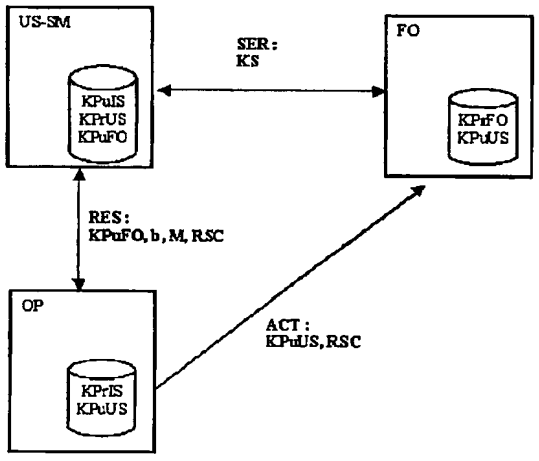
(74) Mandataire : **WENGER, Joel**; Leman Consulting SA, Route de Clémenty 62, CH-1260 Nyon (CH).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH,

[Suite sur la page suivante]

(54) Title: METHOD FOR ALLOCATING SECURED RESOURCES IN A SECURITY MODULE

(54) Titre : METHODE D'ALLOCATION DE RESSOURCES SECURISEES DANS UN MODULE DE SECURITE



(57) Abstract: The aim of the invention is to provide a method for allocating resources in a security module of a mobile device such as a telephone, which takes into account the security imperatives of the different parties such as the operator and the application suppliers. To this end, the invention relates to a method for allocating resources of a security module of an appliance connected to a network, said network being administered by an operator and said resources being used by application suppliers. The inventive method consists of the following steps: a pair of asymmetric keys is generated and the private key is stored in the security module, the public key being stored with the operator; at least one public key pertaining to the operator is introduced into the security module; the operator receives a request from a supplier, said request comprising at least the public key of the supplier; an instruction for reserving a resource is transmitted by the operator towards the security module, along with the public key of the supplier; the operator transmits the public key of the security module to the supplier; and a secured communication is established between the supplier and the security module.

[Suite sur la page suivante]

WO 2004/114229 A1

PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **États désignés** *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) **Abrégé :** Le but de la présente invention est de proposer une méthode pour allouer des ressources sur un module de sécurité d'un appareil portable tel qu'un téléphone et qui tienne compte des impératifs de sécurité des différents intervenants tels que l'opérateur et les fournisseurs d'applications. Ce but est atteint par une méthode d'allocation de ressources d'un module de sécurité d'un appareil connecté à un réseau, ce réseau étant administré par un opérateur, lesdites ressources étant utilisées par des fournisseurs d'application, cette méthode consistant dans les étapes suivantes: génération d'une paire de clés asymétriques et stockage de la clé privée dans le module de sécurité, la clé publique étant stockée chez l'opérateur, introduction d'au moins une clé publique de l'opérateur dans le module de sécurité, réception par l'opérateur d'une requête d'un fournisseur, cette requête comprenant au moins la clé publique du fournisseur, transmission par l'opérateur d'une instruction de réservation d'une ressource vers le module de sécurité accompagnée par la clé publique du fournisseur, transmission par l'opérateur de la clé publique du module de sécurité au fournisseur, établissement d'une conununication sécurisée entre le fournisseur et le module de sécurité.